UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,732	02/27/2001	Wilhelmus Gerardus Petrus Mooij	82032-0005	9900

21186 7590 04/03/2006	EXAMINER	
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH	COLIN, CARL G	
1600 TCF TOWER		
121 SOUTH EIGHT STREET	ART UNIT	PAPER NUMBER
MINNEAPOLIS, MN 55402	2136	

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
Office Action Summary	09/763,732	MOOIJ ET AL.
	Examiner	**Art Unit**	
	Carl Colin	2136	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 January 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-15</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-15</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on <u>02 December 2004</u> is: a)☒ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1.   In response to communications filed on 1/24/2006, applicant has amended claims 1 and

3. The following claims 1-15 are presented for examination.

2.   In response to communications filed on 1/24/2006, the objection to the claims and the

112 rejection has been withdrawn.

3.   Applicant's arguments, pages 6-17, filed on 1/24/2006, with respect to the rejection of

claims 1-15 have been fully considered, but they are not persuasive as amended. In view of

claims 3 and 10, Applicant misinterprets the Office Action by stating that the virtual device

driver corresponds to the secure device and decryption device to show that the device driver does

not establish communication interface between the secure device and a decryption device.

Examiner asserts that the device driver is not interpreted as a secure device (see office action)

therefore, applicant's argument is erroneous, and the secure device driver does establish a

communication interface between the player and the secure device (see figures 6-7); more

clarification and detailed explanation is provided below in the Office Action. Claim 1 recites

similar limitations as explained above. Applicant has amended the claims to recite that the

secure device is arranged to transform the secure device data into information required to decrypt

the encrypted data this limitation was already addressed in the last office action. With respect to

the 103 rejection in view of Shear, applicant argues that the references cannot be combined

because they are contracditory. Examiner respectfully disagrees. The Office action clearly shows that the claimed limitation is obvious over the prior art. Applicant has not addressed the citation provided in the office action, instead applicant is relying to different embodiments to argue that the references cannot be combined. In view of the above and in the Office action, applicant has not overcome the prior art and the claims remain rejected in view of the same references.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1   **Claims 3** and **10** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent

6,052,780 to **Glover**.

4.2   **As per claims 3 and 10, Glover** discloses a method and system for decrypting encrypted

data in a DVD player or computer system (content player), comprising an input for receiving

digital information (protected contents) (see column 6, line 54 through column 7, line 5),

containing encrypted hidden information (encrypted data), keys, passwords, identifiers,

encryption/decryption algorithms... (secure device data); labels and location. **Glover** also

discloses the secure protected content contains an unwrap procedure identifying a virtual device

driver for communication between the DVD player (content player) and a secure disk (secure

device) (column 9, lines 5-52, column 7, lines 15-47, and column 11 and (figures 6-7) that meets

the recitation of information on a protocol for communication between the content player and a

secure device, for example (see column 9, lines 5-52 and column 10, lines 1-27), and unwrap

procedure using tags (attribute data) on the different parts inside the protected contents (column

9, lines 5-52 and column 10, lines 1-27 and lines 60-67); a decryption device (see column 6, lines

54-67) and a processor executing an operating system that meets the recitation of a control

device (see column 6, lines 34-54); wherein said secure device data comprises information

required to decrypt the encrypted data (column 9, lines 5-52 and column 10, lines 1-27; and

column 21, lines 54-67); and discloses unwrap procedure that contains information to locate the

appropriate device driver for establishing a communication interface for communication between

the DVD player and a secure disk for retrieving the information to decrypt the encrypted data

(see column 10, lines 1-27 and column 21, lines 5-52) that meets the recitation of wherein the

attribute data comprises information to find in the protected contents information on the

appropriate protocol for communication between the decryption device and a secure device for

retrieving the information to decrypt the encrypted data. **Glover** discloses wherein the control

device is programmed to use said protocol information to establish a communication interface

(device driver) between the decryption device and a secure device used with the content player

wherein the decryption device is suitable for communicating with the secure device as controlled

by the protocol information to obtain information required to decrypt the encrypted data (see

column 6, line 34 through column 7, line 5; and columns 10-11 and column 19, line 43 through

column 20, line 3). **Glover** discloses the secure device such as the disk arranged to transform the

secure device data into information required to decrypt the encrypted data, wherein the secure

device data comprises the information required to decrypt the encrypted data (see column 21).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

5.1   **Claims 1, 2,** and **15** are rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent 6,052,780 to **Glover**.

        As per claims 1 and 15, Glover discloses a system for providing encrypted data to be

used in a content player comprising an encryption device for encrypting data using an encryption

algorithm (column 3, lines 35-51). **Glover** discloses embodiments for decrypting and executing

the protected contents but does not explicitly disclose detail embodiment about the encryption

process. Claims 1 and 15 recite similar limitations as claims 3 and 10 except for implementing

the invention in encryption mode, which is the reverse of the decryption steps of claims 3 and 10.

It would have been obvious to one skilled in the art to make such modification because it

requires routine skilled in the art to change encryption to decryption or vice-versa. As reciting in

claim 15, **Glover** also discloses the present invention can be used for on-line or live use of digital

information that meets the recitation of broadcasting the protected contents (see column 22, lines

1-20) and discloses providing secure device data, and providing information on a protocol for

communication between the content player and a secure device, (column 9, lines 5-52 and

column 10, lines 1-27 and lines 60-67); and providing a protected contents containing the

encrypted data the secure device data, said protocol information and attribute data on the

different parts inside the protected contents, wherein said secure device data comprises

information required to decrypt the encrypted data (column 9, lines 5-52 and column 10, lines 1-

27; and column 21, lines 54-67), and wherein the attribute data comprises information to find in

the protected contents information on the appropriate protocol for establishing a communication

interface between the content player and the secure device for retrieving the information to

decrypt the encrypted data (see column 10, lines 1-27 and column 21, lines 5-52; column 6, line

34 through column 7, line 5; and column 10). **Glover** discloses the secure device such as the

disk arranged to transform the secure device data into information required to decrypt the

encrypted data, wherein the secure device data comprises the information required to decrypt the

encrypted data (see column 21). Claims 1 and 15 recite similar limitations as found in claims 3

and 10 and therefore they are also rejected on the same rationale as in the rejection of claims 3

and 10.

As per claim 2, Glover discloses providing a device driver that meets the recitation of

secure device applet containing information on a protocol for communication (column 11, lines

59-65) the device driver is also provided with the protected contents as explained above and

provided by protection device in the service provider as part of the encryption process (see

column 21, lines 5-17 and line 45 through column 22, line 20).

6.   **Claims 4-9** and **11-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent 6,052,780 to **Glover** in view of US Patent 6,157,721 to **Shear et al**.

6.1   **As per claims 4, 5, 11, and 14, Glover** substantially discloses a device driver as

appropriate protocol information for communication between the content player and the secure

device provided as a secure device applet (column 11) wherein the processor executing the

operating system is programmed to operate as a virtual machine to execute the secure device

applet to establish said communication interface (see column 6, line 34 through column 7, line 5

and column 10). **Glover** also suggests authentication and authorization procedures to use the

device driver (column 14, lines 35-50 and column 10, lines 1-18) and using any kind of

encryption decryption for security and preventing the risk of virus (column 8, lines 61-63,

column 3, lines 19-33, column 21, lines 54-67). **Glover** is directed more into making sure that

the user environment is authorized to use the driver and does not explicitly disclose

authenticating the device driver (applet) for verifying also that only a verified secure driver is

loaded into the machine. **Shear et al** in an analogous art discloses a load module (column 3,

lines 15-35 and column 8, line 14-50; column 14, lines 39-60; and column 20, lines 1-48) as

protected content containing digital signature, keys, specifications, and other load module

(secure device applet) (column 2, lines 27-65) wherein the control device comprises an applet

loader for verifying the authentication of a secure device applet, wherein only a verified secure

device applet is loaded into the virtual machine (column 5, lines 25-67 and column 6, lines 5-62;

and column 14, lines 39-60). **Shear et al** discloses providing a load module as a secure device

applet, wherein the protected processing environments provide secure execution environment

programmed to operate as a virtual machine to execute the secure device applet to establish said

communication interface, for example (see column 8, line 14-67 and column 5, lines 25-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the method of Glover to also provide authentication of a secure device ap-

plet, wherein only a verified secure device applet is loaded into the virtual machine as suggested

by **Shear et al** for securing the user protected processing environment against inauthentic applet

and to ensure that the applet is intact and was created by a trusted source (see column 4, lines 22-

50). One skilled in the art would have been lead to make such a modification to encrypt and

authenticate applet whenever they are shared because it would prevent attacks on the user

computer/player and secure the user computer/player against inauthentic applet and also ensure

that the applet is intact and was created by a trusted source as suggested by **Shear et al** (see

column 4, lines 22-50).

As per claim 6, Glover discloses the limitation of wherein at least one secure device

applet in the protected contents is encrypted, wherein the applet loader is adapted to decrypt an

encrypted secure device applet, for example (see column 18, line 56 through column 19, line 14

and line 19 through column 20, line 10 and column 20, lines 35-53).

As per claim 7, Glover discloses the limitation of wherein the virtual machine comprises

a content player application program interface and a security application program interface, the

secure device applet communicating with the content player and the secure device by means of

said interfaces, for example (see column 10, line 48 through column 11, line 26 and column 6,

line 54 through column 7, line 5).

As per claims 8 and 12, the combination of **Glover** and **Shear** discloses the limitation of

wherein the control device is arranged to determine the type of secure device used in the

system/player, wherein the control device is arranged to retrieve a secure device applet from the

protected contents corresponding with the type of secure device, for example (see **Shear,** column

16, lines 37-44 and column 18, line 32 through column 19, line 32; see also column 20, line 26

through column 21, line 7). Claims 8 and 12 are also rejected on the same rationale as in the

rejection of claims 4, 5, and 11.

As per claims 9 and 13, the combination of **Glover** and **Shear** discloses the limitation of

wherein the system is part of a content player connected to a network, wherein the control device

is arranged to determine the type of secure device used in the system, and wherein the control

device is arranged to request a corresponding secure device applet to be downloaded from a

service provider, for example (see **Shear**, column 16, lines 37-44; and column 18, line 32

through column 19, line 32; see also column 20, line 26 through column 21, line 7).

Conclusion

7.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

7.1   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure as the art discloses secure content delivery system providing an applet as an interface

for controlling the decryption of the content.

US Patents: 6,418421 Hurtado et al; 6,055,314 Spies et al ; 5,953,005 Liu ;   6,005,942 Chan

et al.

7.2   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
March 27, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100